대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0083112
Application Number

출 원 년 월 일 : 2002년 12월 24일
Date of Application DEC 24, 2002

출 원 인 : 학교법인 한국정보통신학원
Applicant(s) INFORMATION AND COMMUNICATIONS UNIVERSITY EDUCATION/

2003 년 03 월 05 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2002.12.24
【발명의 명칭】	겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법
【발명의 영문명칭】	METHOD OF ID-BASED BLIND SIGNATURE BY USING BILINEAR PARINGS
【출원인】	
【명칭】	학교법인 한국정보통신학원
【출원인코드】	2-1999-038195-0
【대리인】	
【성명】	장성구
【대리인코드】	9-1998-000514-8
【포괄위임등록번호】	2000-005740-6
【대리인】	
【성명】	김원준
【대리인코드】	9-1998-000104-8
【포괄위임등록번호】	2000-005743-8
【발명자】	
【성명의 국문표기】	장 팡구오
【성명의 영문표기】	ZHANG,Fangguo
【주소】	대전광역시 유성구 화암동 58-4
【국적】	CN
【발명자】	
【성명의 국문표기】	김광조
【성명의 영문표기】	KIM,Kwang Jo
【주민등록번호】	560410-1347622
【우편번호】	302-773
【주소】	대전광역시 서구 둔산동 삼성한마루아파트 7-1406
【국적】	KR
【심사청구】	청구
【조기공개】	신청

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 심사청구 , 특허법 제64조의 규정에 의한 출원공개를 신청합니다. 대리인
장성구 (인) 대리인
김원준 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	0	면	0 원
【우선권주장료】	0	건	0 원
【심사청구료】	10	항	429,000 원
【합계】	458,000 원		
【감면사유】	학교		
【감면후 수수료】	229,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통 2.고등교육법 제2조에의한 학교임을 증명하는 서류[설립인가서]_1통

【요약서】

【요약】

본 발명은 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법에 관한 것으로, 은닉 서명을 위해 시스템 매개변수를 생성하는 단계; 개인 식별 정보를 갖는 사용자 및 서명자의 공개키와 비밀키를 계산하는 단계; 서명자가 위탁 값을 계산하여 사용자에게 전송하는 단계; 사용자가 위탁 값에 대한 은닉 값을 계산하여 서명자에게 전송하는 단계 ; 은닉 값에 대하여 서명자가 자신의 비밀키를 이용하여 서명 값을 계산하여 사용자에게 전송하는 단계; 서명 값으로부터 은닉 값을 제거하여 은닉 서명을 복구하는 단계; 은닉 서명의 정당성을 검증하는 단계를 포함한다. 따라서, 인증서 기반의 공개키 기반 구조가 가지고 있는 많은 연산량과 통신량을 효과적으로 축소하기 위하여 개인식별정보 기반의 공개키 기반 구조가 활발하게 연구되고 있으며 공개키 기반 구조를 포함한 다양한 응용에서 개인식별정보 기반의 은닉서명은 필수요소이며 응용성이 아주 우수하다는 효과가 있다.

【대표도】

도 2

【명세서】

【발명의 명칭】

겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법{METHOD OF ID-BASED BLIND SIGNATURE BY USING BILINEAR PARINGS}

【도면의 간단한 설명】

도 1은 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법을 수행하기 위한 블록 구성도이고,

도 2는 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법에 대한 상세 흐름도이다.

<도면의 주요부분에 대한 부호의 설명>

100 : 서명자 200 : 사용자

300 : 신뢰기관(또는, 키생성 센터)

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 본 발명은 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법에 관한 것으로, 특히 전자 화폐나 전자 투표 시스템 등에서 사용되는 메시지의 내용을 모르고 서명문을 생성하는 은닉서명에 있어서, 겹선형 쌍(Bilinear Pairings)을 이용하여 사용의 개인식별정보에 기반하고 있는 암호학적으로 안전하게 하는 은닉서명 방법에 관한 것이다.

<7> 통상적으로, 정보통신망의 발전과 더불어 다양한 정보가 사이버 공간을 통하여 전달 및 가공되고 있는 실정이다. 송신자가 전자 우편이나 전자 문서 전달 시스템 등을 통하여 귀중한 메시지를 전달하고자 할 때, 메시지 송신자의 입장에서는 정당한 수신자가 정보를 제대로 받았는지, 그리고 수신자의 입장에서는 메시지의 생성자가 정당한 송신자가 맞는지 등을 확인할 메커니즘이 필요하다.

<8> 이러한 기능을 효과적으로 제공하기 위한 방법 중의 하나로 각 사용자가 2개의 키 정보로서 비밀키와 공개키를 가지고 있는 공개키 암호 시스템을 이용한 전자 서명 방식이 이용되고 있다.

<9> 즉, 전자서명은 인터넷 기반의 거래나 전자상거래 등에 있어서 가장 메시지의 인증이나 부인 방지 등에 중요하게 사용되며 특히, 은닉전자서명(Blind Digital Signature) 또는 간단히 은닉서명(Blind Signature)은 전자서명에 추가 요구사항과 기능이 덧붙여진 매우 중요한 서명기법이다.

<10> 은닉서명의 개념은 네덜란드 암호학자 촘(Chaum)에 의해서 최초로 1983년에 제안되었으며, 전자현금, 전자투표 등의 응용 시스템에서 사용자에게 익명성을 제공한다. 일반 전자서명과 달리, 은닉서명은 사용자와 서명자간의 2자간 대화형 프로토콜이라 볼 수 있다.

<11> 은닉서명을 이용해 사용자는 서명자가 메시지와 서명 결과에 대한 정보를 얻을 수 없는 메시지의 서명값을 얻을 수 있다. 은닉서명은 전자서명의 인증성을 제공하는 동시에 익명성을 보장하는 매우 중요한 기능을 담당한다.

<12> 공개키 시스템에서, 각 사용자는 공개키와 비밀키 쌍을 갖는다. 사용자의 공개키와 개인식별정보는 전자 인증서(Digital Certificate)에 의해서 소유주와 연결된다. 이를 연결하기 위한 사회적인 기반 구조인 공개키 기반구조(Public Key Infrastructure, PKI)는 복잡하고 계층적인 인증기관의 유지, 막대한 통신비용 및 인증서 확인을 위해 요구되는 계산비용 등에 막대한 경비가 소요된다.

<13> 그러나 모든 인증서는 공개되어 있고 모든 사용자가 쉽게 접근할 수 있다는 것이 기본적인 가정하에 공개키 기반 구조는 사용될 수 있으나, 이것은 모든 통신 환경에서 용이한 것만은 아니다. 특히, 무선망에서 네트워크의 연결은 간헐적일 수가 있으며 인증서 기반 시스템에서 사용자의 공개키를 사용하기 전에 프로토콜 참여자는 먼저 그 사용자의 인증서를 확인해야 한다. 결국, 이러한 시스템은 많은 계산시간과 사용자 증가에 따라 방대한 양의 저장 공간을 요구한다.

<14> 공개키 암호시스템(Public Key Cryptosystem, PKC)에서의 공개키 관리의 비용을 해소하기 위하여, 샤미르(Shamir)는 1984년에 누구든지 쉽게 구성할 수 있는 개인식별정보(IDentity Information) 기반의 공개키 암호시스템이나 개인 식별 방식을 구성할 수 있는 새로운 개념을 제안했다.

<15> 개인식별정보 기반 공개키 암호는 개인식별정보와 공개키 간의 일대일 사상으로 구성하여 사용할 수 있다. 그래서 개인식별정보 기반 암호는 기존의 공개키 인증서와 인증기관에 대한 필요성뿐 만 아니라 의존성도 크게 줄였다. 개인식별정보 기반 암호는 전자우편 주소나 전화번호 같은 임의의 식별값으로부터 공개키를 유도할 수 있기 때문에 공개키 암호를 도입하거나 공개키 암호로 이전하는 것이 쉽게 할 수 있도록 하는 유용한 암호학적 도구이다. 동시에 개인식별정보 기반 방법은 공개키 인증서의 필요성과 수를

줄일 수 있도록 하기 때문에 키 관리 문제가 대단히 용이하다. 개인식별정보 기반의 공개키 환경은 인증서 기반 공개키 환경의 대안이 될 수 있다. 특히 효율적인 키 관리와 안전성에 대한 요구가 강하지 않은 경우 특히 그러하다.

<16> 겹선형쌍(Bilinear pairs), 예를 들면, 대수 곡선의 웨일(Weil) 쌍과 테이트(Tate) 쌍은 대수기하학 연구에서 매우 중요한 도구들이다. 암호 시스템에서 겹선형 쌍 성질의 초기 응용은 이산대수문제(Discrete Logarithm Problem)의 계산 어려움을 평가를 위한 곳에 이용되었다. 예를 들면, 웨일 쌍을 사용한 엠오브이(MOV) 공격이나 테이트 쌍을 이용한 에프알(FR) 공격은 특정 타원곡선이나 초타원곡선에서의 이산대수문제를 확장 유한체에서의 이산대수문제로 근사되어 문제해결이 용이하게 할 수 있는 데 이용되었다. 2001년도에 겹선형 쌍들이 암호에서 다양한 응용분야가 있다는 것이 밝혀졌는 데, 보네(Boneh)와 프랭크린(Franklin)의 개인식별정보 기반 암호 시스템, 스마트(Smart)의 개인식별정보 기반 인증 키관리 관리와 몇 가지 개인식별정보 기반 전자서명 기법을 들 수 있다.

<17> 개인식별정보 기반의 은닉서명은 일반 은닉서명과 개인식별정보 기반 기법을 결합한 것으로 은닉서명의 검증을 하기 위한 공개키가 서명자의 개인식별정보가 되는 것이다. 개인식별정보 기반 은닉서명은 서명자의 공개키가 단순히 그의 개인식별정보이기 때문에 유용하다. 예를 들면, 은행이 개인식별정보 기반의 은닉서명을 가지고 전자현금을 발행하는 경우 사용자나 전자상점은 데이터베이스에서 은행의 공개키를 가져올 필요가 없다. 즉, 국가명, 도시명, 은행이름, 해당년도 등의 연접 정보를 통해서 당해연도에 발행된 전자현금을 쉽게 검증할 수 있다.

<18> 보네와 프랭크린에 의한 최초 제안에는 겹선형성 사상을 갖는 군(Group)의 특성을 사용한 암호 시스템의 구성 방법이었으며 그 이후 키합의 및 키 동의 기법, 서명기법 등이 제안되었으나 개인식별정보 기반의 공개키 구조에서 필수적인 개인식별정보 기반의 은닉서명 기법은 현재까지 제안되어 있지 아니하다는 문제점이 있었다.

【발명이 이루고자 하는 기술적 과제】

<19> 따라서, 본 발명은 상술한 문제점을 해결하기 위해 안출한 것으로서, 그 목적은 개인식별정보 기반 공개키 암호시스템의 필수 항목의 하나인 개인식별정보 기반 은닉서명 기법을 웨일 쌍이나 테이트 쌍과 같은 겹선형 쌍을 사용하여 안전성과 익명성을 제공하는 새로운 개인식별정보 기반 은닉서명 기법을 제안할 수 있도록 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법을 제공함에 있다.

<20> 상술한 목적을 달성하기 위한 본 발명에서 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법은 은닉 서명을 위해 시스템 매개변수를 생성하는 단계; 개인 식별 정보를 갖는 사용자 및 서명자의 공개키와 비밀키를 계산하는 단계; 서명자가 위탁 값을 계산하여 사용자에게 전송하는 단계; 사용자가 위탁 값에 대한 은닉 값을 계산하여 서명자에게 전송하는 단계; 은닉 값에 대하여 서명자가 자신의 비밀키를 이용하여 서명 값을 계산하여 사용자에게 전송하는 단계; 서명 값으로부터 은닉 값을 제거하여 은닉 서명을 복구하는 단계; 은닉 서명의 정당성을 검증하는 단계를 포함하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<21> 이하, 첨부된 도면을 참조하여 본 발명에 따른 일 실시 예를 상세하게 설명하기로 한다.

<22> 도 1은 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법을 수행하기 위한 블록 구성도로서, 도 1a는 은닉서명 기법의 주 참여자인 서명자(100)와, 사용자(200) 및 신뢰기관(300)을 포함한다.

<23> 서명자(100)는 주어진 시스템 매개변수에 따라 신뢰기관(300)이 제공하는 공개키와 비밀키를 사용하여 사용자(200)가 요구하는 메시지에 대하여 메시지의 내용을 모른 체 은닉서명을 계산하여 사용자(200)에게 전송하는 역할을 담당한다.

<24> 사용자(200)는 서명자(100)에게 제시할 메시지를 은닉하고 서명자(100)로부터 제공받은 은닉서명에 대한 서명을 계산하는 역할을 담당한다. 사용자(200)의 메시지와, 서명자(100)가 제시한 은닉서명에서 추출한 서명 값으로부터 정당성을 검증할 수 있다.

<25> 신뢰기관(300)은 각 참여자가 모두 사용할 수 있는 시스템 매개변수를 생성하여 공개하고 각 참여자의 신원 값을 바탕으로 각각의 공개키와 비밀키를 생성하여 안전한 채널로 제공하는 역할을 담당한다. 여기서, 신뢰기관(300)은 시스템 초기화 시에만 참여하고 서명에는 참여하지 않는다.

<26> 도 1a 내지 도 1c에 대하여 보다 상세하게 설명하면, 상술한 참여자(서명자(100), 사용자(200), 신뢰기관(300))로 구성된 본 발명의 은닉서명 기법은 도 1a의 시스템 매개변수와 마스터 키 생성과정 및 서명자(100)의 공개키와 비밀키 생성과정과, 도 1b의 서명자(100)와 사용자(200)간에 위탁, 메시지 은닉, 서명 및 서명 검증 과정과, 도 1c의 사용자(200)가 서명자(100)의 서명의 유효성을 검증하는 과정을 통하여 동작하는 것으로, 본 발명은 사용자(200)가 서명자(100)의 서명을 최종적으로 확인하는 기법과 관련된다.

<27> 도 2의 흐름도를 참조하면서, 상술한 구성을 바탕으로 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법에 대하여 보다 상세하게 설명한다.

<28> 먼저, 시스템 매개변수 생성과정으로서, 서명자(100) 및 사용자(200) 모두가 공유하는 시스템 매개변수들이 신뢰기관(300)에 의해서 생성되어 공개된다(단계 201).

<29> 이러한 과정에서 임의의 순환군 G 와 V 가 생성되며, G 와 V 의 위수는 모두 q 이다. 순환군 G 에 대한 임의의 생성자 P 을 생성하며, 끝으로, 두 순환군 G와 V에 대한 겹선형 사상 e 를 수학식 1과 같이 정의한다.

<30> 【수학식 1】 $e:G\times G\mapsto V$

<31> 여기서, G 는 타원 곡선군 또는 초타원 곡선 자코비언(Jacobian)이며, V 는 곱셈 순환군 Z_q^*을 사용한다.

<32> 다음으로, 신뢰기관(300)은 마스터키로 Z_q^* 에 속하는 임의의 정수 s 을 선택하고 $P_{pub}=sP$을 계산한다. 추가로 수학식 2의 사상을 만족하는 암호학적 해시 함수 H,H_1 을 생성한다.

<33> 【수학식 2】 $H:\{0,1\}^*\mapsto Z_q^*,H_1:\{0,1\}^*\mapsto G$

<34> 즉, $H:\{0,1\}^*\mapsto Z_q^*$ 와 $H_1:\{0,1\}^*\mapsto G$ 을 선택하는 것이다.

<35> 그 다음 단계로서, 신뢰기관(300)은 시스템 매개변수로서 $<G,q,P,P_{pub},H,H_1>$ 을 공개하고 s 을 마스터키로 사용하며, 시스템 매개변수와 마스터키를 사용하여 사용자(200)의 개인식별정보를 사용하여 신뢰기관(300) 자신의 공개키 P_{pub} 를 수학식 3을 사용하여 계산한다(단계 202).

<36> 【수학식 3】 $P_{pub}=s \cdot P$

<37> 이후, 신뢰기관(300)은 신원값으로 개인식별정보를 갖는 사용자(200)가 비밀키와 공개키 생성을 요청하면, 수학식 4를 사용하여 해당 사용자(200)의 공개키 Q_{ID} 를 생성하고, 수학식 5를 사용하여 비밀키 S_{ID} 를 생성하여 안전한 채널로 전송한다(단계 203).

<38> 【수학식 4】 $Q_{ID}=H_1(ID)$

<39> 【수학식 5】 $S_{ID}=s \cdot Q_{ID}$

<40> 여기서, 신원 값 개인식별정보를 갖는 사용자(200)의 공개키는 $Q_{ID}=H_1(ID)$ 이며 비밀키는 $S_{ID}=sQ_{ID}$ 이다.

<41> 다음으로, 은닉서명 과정으로, 은닉서명을 얻고자 하는 메시지를 m 이라 한 다음에, 신뢰기관(300)이 공개한 시스템 매개변수를 바탕으로 서명자(100)가 Z_p^* 에 속하는 임의의 난수 r 을 선택하여 수학식 6을 사용하여 위탁할 값 R 을 계산하여 사용자(200)에게 전송한다(단계 204).

<42> 【수학식 6】 $R=r \cdot P$

<43> 그 다음으로, 사용자(200)는 먼저 은닉인수에 해당하는 a,b 를 Z_q^* 에서 선택하여 수학식 7을 사용하여 은닉서명을 받으려는 은닉 메시지 c 를 계산하여 서명자(100)에게 전송한다(단계 205).

<44> 【수학식 7】 $c=H(m,e(b \cdot Q_{ID}+R+a \cdot P,P_{pub}))+b \pmod q$

<45> 그 다음 단계로서, 서명자(100)는 자신의 공개키와 비밀키 쌍을 이용하여 서명값 S 를 수학식 8을 사용하여 계산하여 사용자(200)에게 전송한다(단계 206).

<46> 【수학식 8】 $S=c \cdot S_{ID}+r \cdot P_{pub}$

<47> 사용자(200)는 서명자(100)로부터 은닉 서명 값을 제공받으면 자신의 비밀 값을 사용하여 은닉 값을 제거하고 서명자(100)의 서명 값을 수학식 9와 수학식 10을 사용하여 S',c' 을 복구하여 출력한다(단계 207).

<48> 【수학식 9】 $S'=S+a \cdot P_{Pub}$

<49> 【수학식 10】 $c'=c-b$

<50> 검증하는 과정으로서, 사용자(200)는 자신이 제시한 메시지와, 신뢰기관(300)이 공개한 시스템 매개변수와, 서명자(100)의 공개키 값을 이용하여 서명자(100)가 제공한 은닉서명이 정당한 서명인지를 수학식 11 및 수학식 12를 사용하여 서명을 검증한다(단계 208).

<51> 【수학식 11】 $c'=H(m,e(S',P) \cdot e(Q_{ID},P_{pub})^{-c'})$

<52> 【수학식 12】 $H(m,e(S',P) \cdot e(Q_{ID},P_{pub})^{-c'})$

<53> $=H(m,e(S+aP_{pub},P) \cdot e(Q_{ID},P_{pub})^{-c'})$

<54> $=H(m,e(cS_{ID}+rP_{pub}+aP_{pub},P) \cdot e(Q_{ID},P_{pub})^{-c'})$

<55> $=H(m,e(cS_{ID},P) \cdot e(rP_{pub}+aP_{pub},P) \cdot e(Q_{ID},P_{pub})^{-c'})$

<56> $=H(m,e(S_{ID},P)^{c} \cdot e((r+a)P_{pub},P) \cdot e(Q_{ID},P_{pub})^{-c'})$

<57> $=H(m,e(Q_{ID},P_{pub})^{c} \cdot e((r+a)P,P_{pub}) \cdot e(Q_{ID},P_{pub})^{-c'})$

<58> $=H(m,e(Q_{ID},P_{pub})^{c-c'} \cdot e(R+aP,P_{pub}))$

<59> $=H(m,e(Q_{ID},P_{pub})^{b}\cdot e(R+aP,P_{pub}))$

<60> $=H(m,e(bQ_{ID}+R+aP,P_{pub}))=c-b\,(\mathrm{mod}\,q)=c'$

<61> 상술한 바와 같이, 본 발명에 따른 은닉서명 기법을 이용하면 사용자(200)는 자신의 익명성뿐만 아니라 위조불가능성도 만족하는 효율적인 은닉서명을 자신의 개인식별정보를 이용하는 시스템에서 수행할 수 있다.

<62> 본 발명을 이용하여 은닉서명을 생성하는 경우, 서명자는 그룹 G 상에서 3번의 스칼라 곱셈만 수행하면 되며 사용자는 그룹 G 상에서 3번의 스칼라 곱셈, 1번의 해시 연산, 2번의 겹선형 쌍 연산 및 검증을 수행하는 경우, 1번의 곱셈 순환군 Z_q^* 상에서 1번의 지수승 연산을 요구한다. 이때 겹선형 쌍 연산을 1회 줄일 수 있다. 검증이 자주 일어난다면 다음 수학식 13를 미리 계산하여 놓으면 된다.

<63> 【수학식 13】 $e(Q_{ID},P_{pub})$

<64> 즉, 서명값은 G 와 V 의 원소로 구성되어 지는데, 실제에 있어서는 G 에 속하는 원소의 크기는 헤스(Hess)가 제안한 기법을 사용하여 줄일 수 있으므로, 본 은닉서명은 익명성, 안전성, 위조불가능성을 제공할 뿐만 아니라 연상의 효율성도 얻을 수 있다.

【발명의 효과】

<65> 이상에서 설명한 바와 같이, 본 발명은 겹선형 쌍을 사용하여 개인식별정보 기반의 안전한 은닉서명을 제공함으로써, 인증서 기반의 공개키 기반 구조가 가지고 있는 많은 연산량과 통신량을 효과적으로 축소하기 위하여 개인식별정보 기반의 공개키 기반 구조가 활발하게 연구되고 있으며 공개키 기반 구조를 포함한 다양한 응용에서 개인식별정보 기반의 은닉서명은 필수요소이며 응용성이 아주 우수하다.

<66> 또한, 겹선형 사상을 이용한 본 은닉서명은 기존의 방법과 달리 공개적으로 용이하게 취득할 수 있는 사용자의 개인식별정보를 이용하므로 인증기관에 대한 절대적 의존성을 탈피할 수 있으며, 누구나 개인 식별 정보로 용이하게 검증이 가능하다. 특히 겹선형 사상은 테이트 쌍이나 베일 쌍을 타원곡선 상에서 구현하여 사용하며, 데이트 쌍이나 베일 쌍의 계산이 상대적으로 복잡하여 연산의 비효율성이 지적되어 왔으나, 최근 크립토 2002학회에서 발표한 바레토(Barreto) 등의 연구에 의하면 테이트 쌍이나 베일 쌍의 연산도 매우 효율적으로 계산될 수 있다는 결과의 효과가 있다.

【특허청구범위】

【청구항 1】

개인식별정보 기반의 은닉서명 방법에 있어서,

상기 은닉 서명을 위해 시스템 매개변수를 생성하는 단계;

상기 개인 식별 정보를 갖는 사용자 및 서명자의 공개키와 비밀키를 계산하는 단계;

상기 서명자가 위탁 값을 계산하여 상기 사용자에게 전송하는 단계;

상기 사용자가 위탁 값에 대한 은닉 값을 계산하여 상기 서명자에게 전송하는 단계;

상기 은닉 값에 대하여 상기 서명자가 자신의 비밀키를 이용하여 서명 값을 계산하여 상기 사용자에게 전송하는 단계;

상기 서명 값으로부터 은닉 값을 제거하여 은닉 서명을 복구하는 단계;

상기 은닉 서명의 정당성을 검증하는 단계를 포함하는 것을 특징으로 하는 겹선형 쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 2】

제 1 항에 있어서,

상기 시스템 매개 변수는 신뢰기관에 의해 생성되며, 상기 생성되는 매개 변수 과정에서 임의의 순환군 G 와 V 가 생성되며, 상기 G 와 V 의 위수는 모두 q 이며, 상기 순환군 G 에 대한 임의의 생성자 P 을 생성하며, 상기 순환군G 와 V 에 대한 겹선형 사상 e 를,

수학식 1

$e:G\times G\mapsto V$ 과 같이 정의하며,

여기서, G 는 타원 곡선군 또는 초타원 곡선 자코비언(Jacobian)이며, V 는 곱셈 순환군 Z_q^* 을 사용하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 3】

제 1 항 또는 제 2 항에 있어서,

상기 신뢰기관은 마스터키 s 을 선택하고, 해시 함수 H,H_1 을,

수학식 2

$H:\{0,1\}^*\mapsto Z_q^*,H_1:\{0,1\}^*\mapsto G$ 와 같이 생성하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 4】

제 1 항에 있어서,

상기 시스템 매개변수를 공개하고 마스터키 s 를 사용하여 상기 신뢰기관 자신의 공개키 P_{pub} 를,

수학식 3

$P_{pub}=s\cdot P$ 을 사용하여 계산하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 5】

제 1 항 또는 제 2 항에 있어서,

상기 신뢰기관이 신원값으로 개인식별정보를 갖는 사용자가 비밀키와 공개키 생성을 요청하는 경우,

수학식 4

$Q_{ID}=H_1(ID)$ 을 사용하여 상기 사용자의 공개키 Q_{ID} 를 생성하고,

수학식 5

$S_{ID}=s \cdot Q_{ID}$ 을 사용하여 상기 사용자의 비밀키 S_{ID} 를 생성하여 안전한 채널로 전송하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 6】

제 1 항에 있어서,

상기 서명자가 자신의 위탁 값을 계산할 때, 상기 서명자가 생성한 서명의 위변조를 방지하기 위해 임의의 난수 r을 선택하여 위탁 값 R 을,

수학식 6

$R=r \cdot P$ 을 통해 계산하여 상기 사용자에게 전송하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 7】

제 1 항에 있어서,

상기 사용자가 서명자에게 서명을 요청하는 경우, 익명성을 보장하기 위해 은닉 값을 만들 때, 상기 은닉 값의 위변조를 방지하기 위해 은닉 메시지 c 를,

수학식 7

$c=H(m,e(b \cdot Q_{ID}+R+a \cdot P,P_{pub}))+b \pmod{q}$ 을 통해 계산하여 상기 서명자에게 전송하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 8】

제 1 항에 있어서,

상기 서명자가 서명 값을 계산할 때, 자신의 공개키와 비밀키 쌍을 이용하여 서명 값 S 을,

수학식 8

$S=c \cdot S_{ID}+r \cdot P_{pub}$ 을 통해 계산하여 상기 사용자에게 전송하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 9】

제 1 항에 있어서,

상기 서명자로부터 은닉 서명 값을 제공받은 후, 상기 사용자가 자신의 비밀 값을 사용하여 은닉 값을 제거하고 상기 서명자의 서명 값 S',c' 을,

수학식 9

$S'=S+a \cdot P_{Pub}$

수학식 10

$c'=c-b$ 을 통해 복구하여 출력하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【청구항 10】

제 1 항에 있어서,

상기 은닉 서명의 정당성을 검증하는 단계는,

수학식 11

$$c'=H(m,e(S',P)\cdot e(Q_{ID},P_{pub})^{-c'})$$

수학식 12

$$H(m,e(S',P)\cdot e(Q_{ID},P_{pub})^{-c'})$$

$$=H(m,e(S+aP_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$$

$$=H(m,e(cS_{ID}+rP_{pub}+aP_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$$

$$=H(m,e(cS_{ID},P)\cdot e(rP_{pub}+aP_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$$

$$=H(m,e(S_{ID},P)^{c}\cdot e((r+a)P_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$$

$$=H(m,e(Q_{ID},P_{pub})^{c}\cdot e((r+a)P,P_{pub})\cdot e(Q_{ID},P_{pub})^{-c'})$$

$$=H(m,e(Q_{ID},P_{pub})^{c-c'}\cdot e(R+aP,P_{pub}))$$

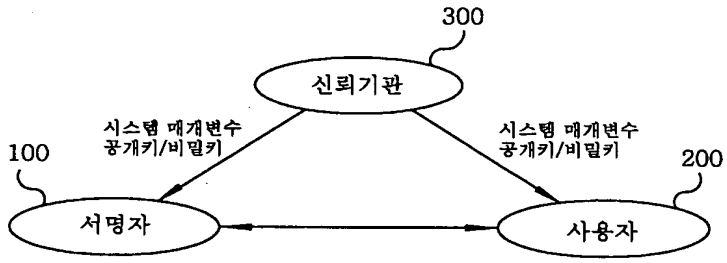
$$=H(m,e(Q_{ID},P_{pub})^{b}\cdot e(R+aP,P_{pub}))$$

$$=H(m,e(bQ_{ID}+R+aP,P_{pub}))=c-b\ (\mathrm{mod}\,q)=c'$$

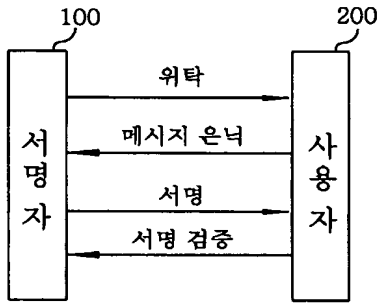
을 통해 검증하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 은닉서명 방법.

【도면】

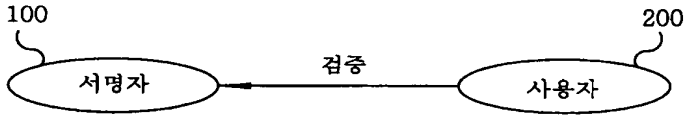
【도 1a】



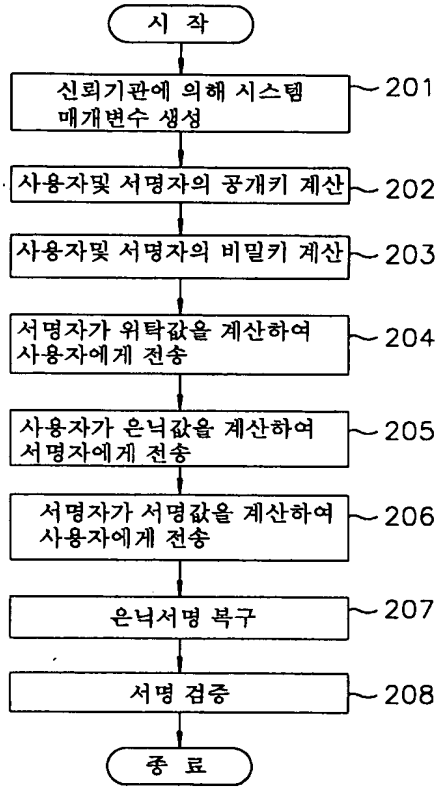
【도 1b】



【도 1c】



【도 2】


시 작
신뢰기관에 의해 시스템 매개변수 생성
201
사용자및 서명자의 공개키 계산
202
사용자및 서명자의 비밀키 계산
203
서명자가 위탁값을 계산하여 사용자에게 전송
204
사용자가 은닉값을 계산하여 서명자에게 전송
205
서명자가 서명값을 계산하여 사용자에게 전송
206
은닉서명 복구
207
서명 검증
208
종 료